INFN-AAI
SAML & OIDC

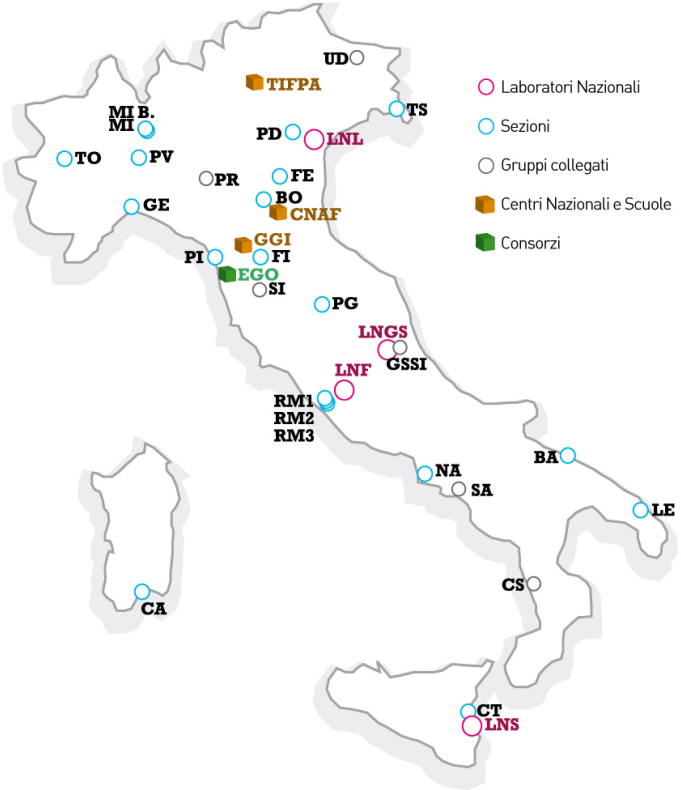
Workshop GARR 2019 – NET Makers

Roma 9 ottobre 2019

Enrico M. V. Fasanelli

Istituto Nazionale di Fisica Nucleare

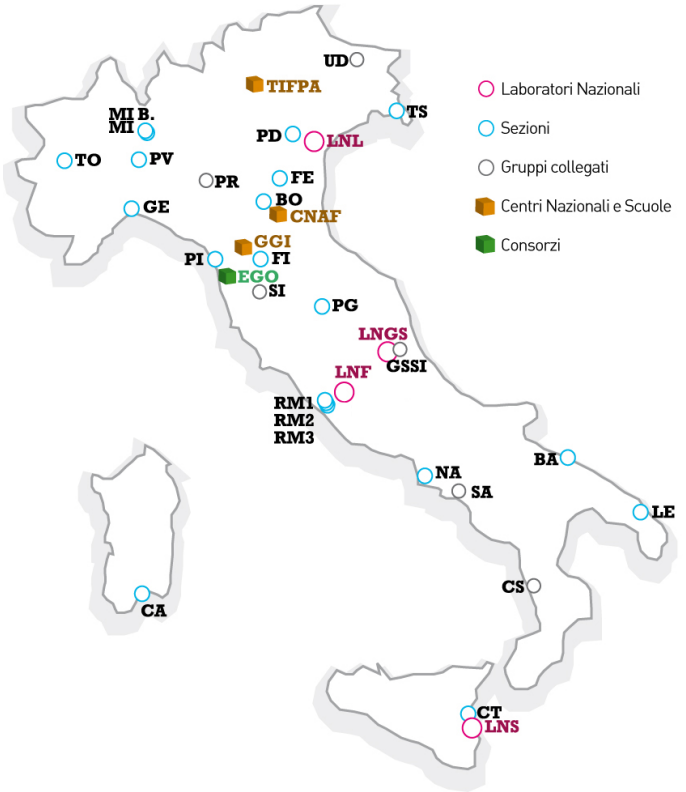
- 26 Sezioni
- 4 Laboratori Nazionali
- 6 Gruppi Collegati
- 3 Centri Nazionali
- Amministrazione Centrale
- Ufficio di Presidenza
- Consorzio EGO



INFN: AuthN & AuthZ pre INFN-AAI (2008)

- 26 Sezioni
- 4 Laboratori Nazionali
- 6 Gruppi Collegati
- 3 Centri Nazionali
- Amministrazione Centrale
- Ufficio di Presidenza
- Consorzio EGO

~41 Strutture
~30 AuthN & AuthZ
>10 DB utenti in AC



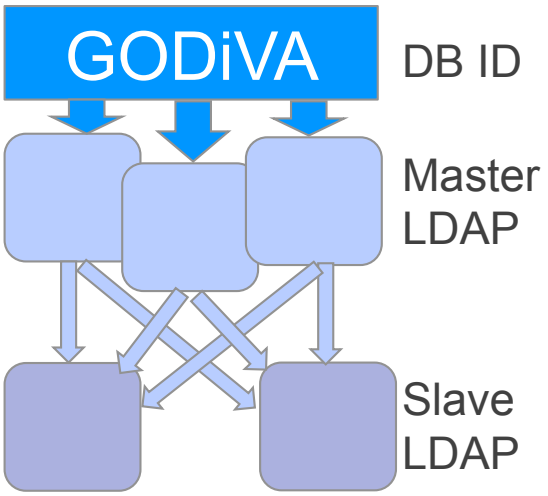
INFN – AuthN & AuthZ con AAI

- Singolo DB Identità Digitali e ruoli
  - DB autoritativo anche per processi amministrativi

GODiVA DB ID

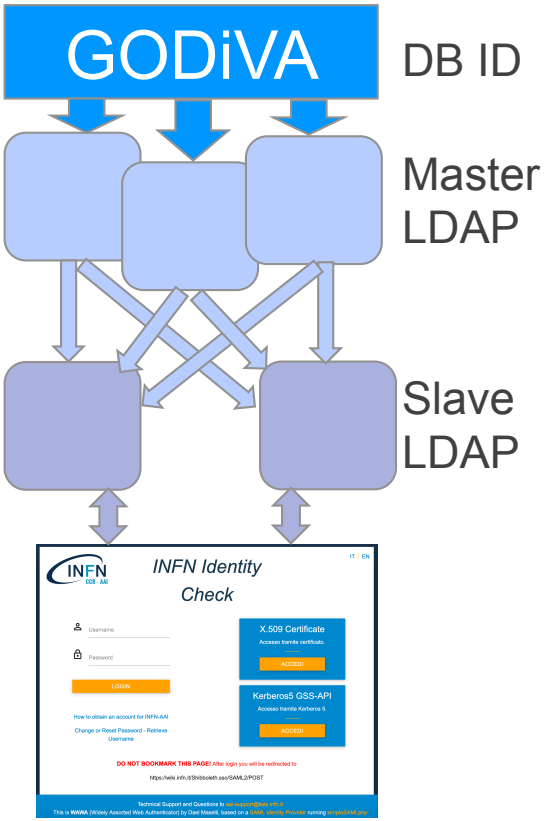
INFN – AuthN & AuthZ con AAI

- Singolo DB Identità Digitali e ruoli
  - DB autoritativo anche per processi amministrativi
- AuthN & AuthZ via LDAP (+Kerberos5)
  - 389-DS multi-master + n slaves
    - 2 master @LNF + 1 master @CNAF
    - 1 slave @LNF + 1 slave @CNAF



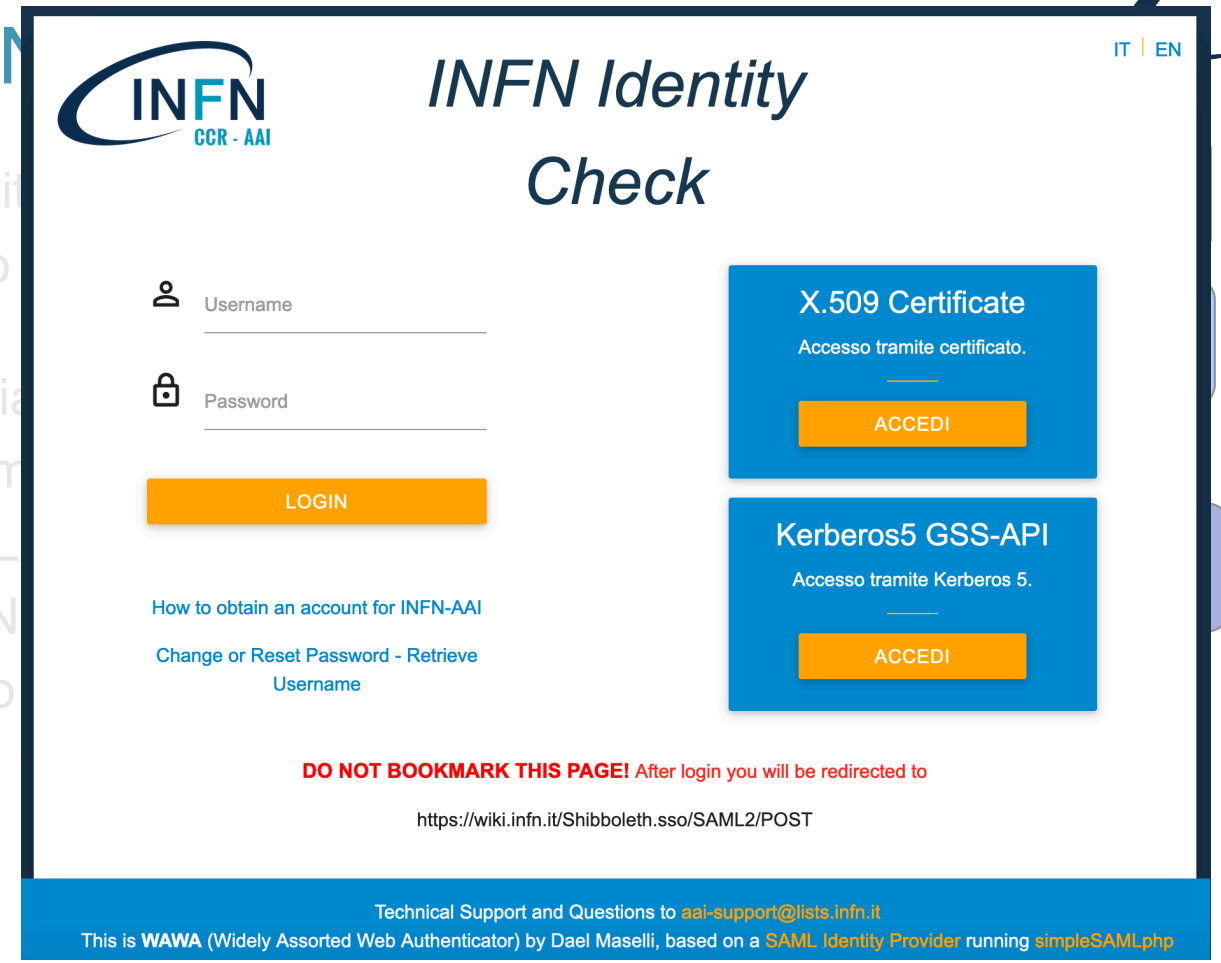
INFN – AuthN & AuthZ con AAI

- Singolo DB Identità Digitali e ruoli
  - DB autoritativo anche per processi amministrativi
- AuthN & AuthZ via LDAP (+Kerberos5)
  - 389-DS multi-master + n slaves
    - 2 master @LNF + 1 master @CNAF
    - 1 slave @LNF + 1 slave @CNAF
- IdP SAML basato su SimpleSAMLphp
  - 2 IdP @LNF + 1 hot-standby @CNAF



INFN – AuthN

- Singolo DB Identit
  - DB autoritativo amministrativi
- AuthN & AuthZ via
  - 389-DS multi-m
    - 2 master @L
    - 1 slave @LN
- IdP SAML basato
  - 2 IdP @LNF +



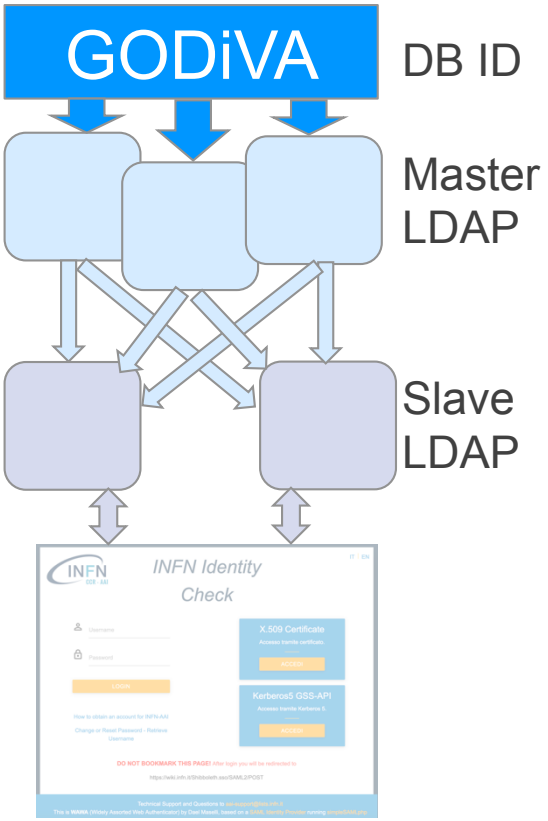
DB ID

Master LDAP

Slave LDAP

INFN – AuthN & AuthZ con AAI

- Singolo DB Identità Digitali e ruoli
  - DB autoritativo anche per processi amministrativi
- AuthN & AuthZ via LDAP (+Kerberos5)
  - 389-DS multi-master + n slaves
    - 2 master @LNF + 1 master @CNAF
    - 1 slave @LNF + 1 slave @CNAF
- IdP SAML basato su SimpleSAMLphp
  - 2 IdP @LNF + 1 hot-standby @CNAF



NonSoloSAML

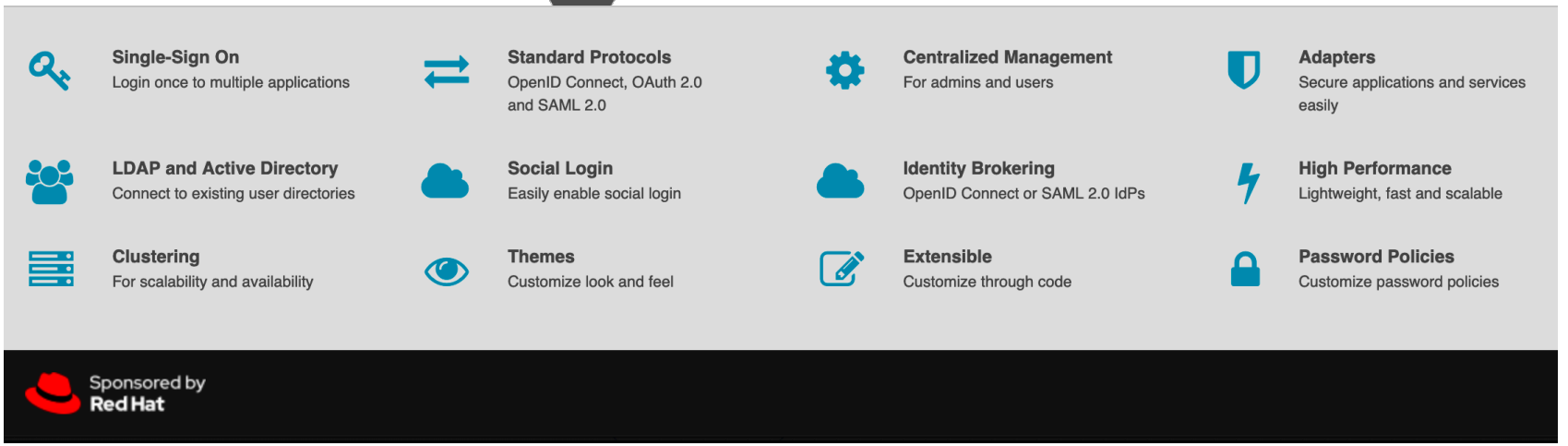
- Sempre più pressante la necessità di supporto per OIDC
- Vincoli: GODiVA e SimpleSAMLphp
  - Provato senza successo il modulo OIDC di RedIRIS

NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincoli: GODiVA e SimpleSAMLphp
  - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in KEYCLOAK

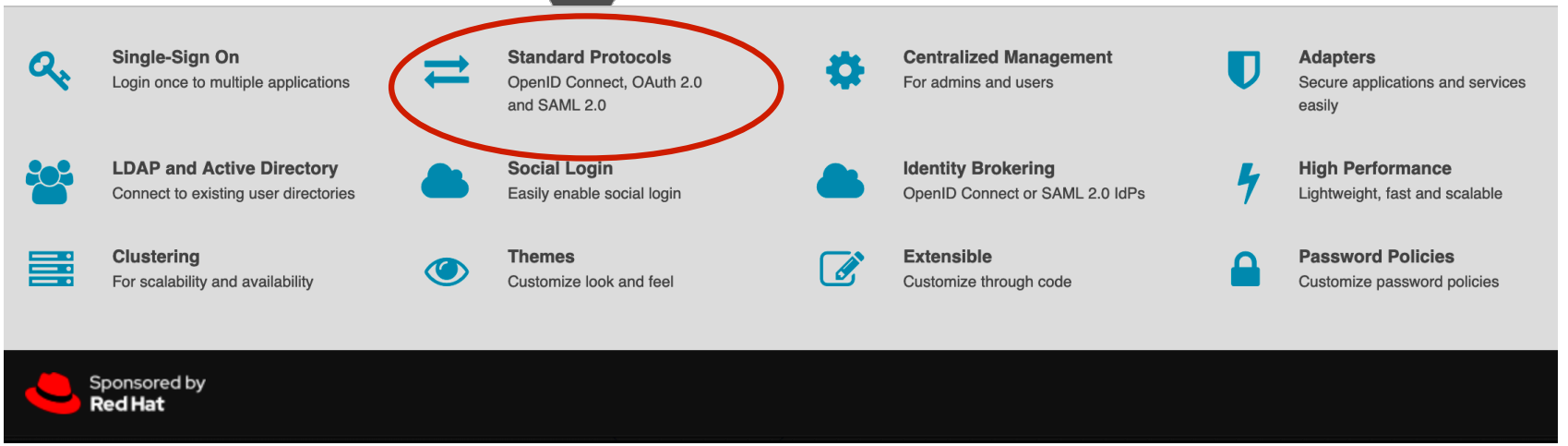
NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincolo: SimpleSAMLphp
  - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in KEYCLOAK



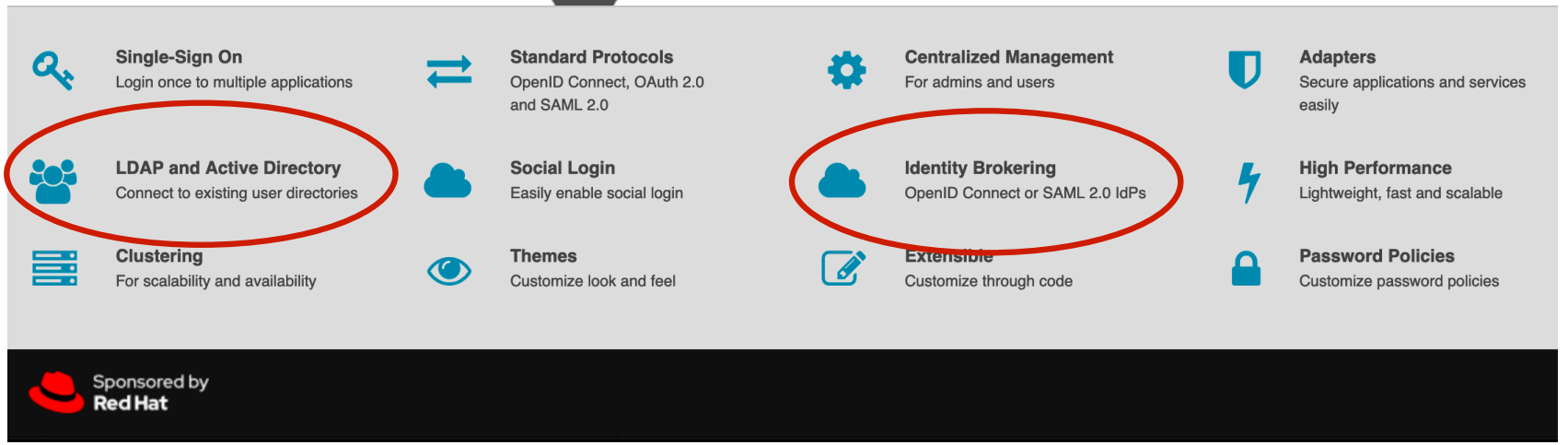
NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincolo: SimpleSAMLphp
  - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in KEYCLOAK



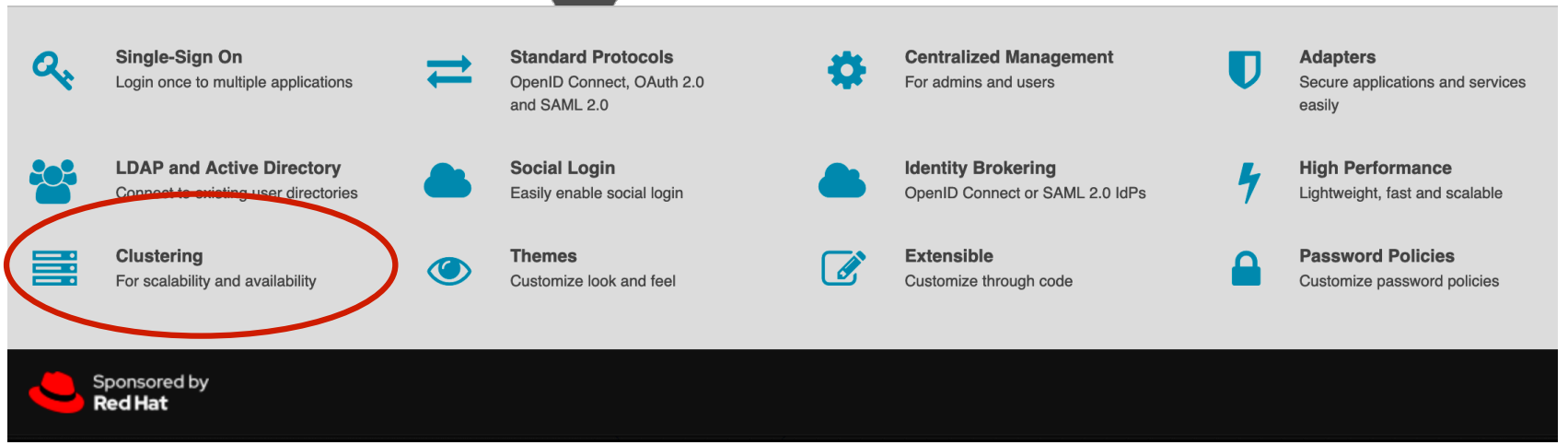
NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincolo: SimpleSAMLphp
  - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in KEYCLOAK



NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincolo: SimpleSAMLphp
  - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in KEYCLOAK

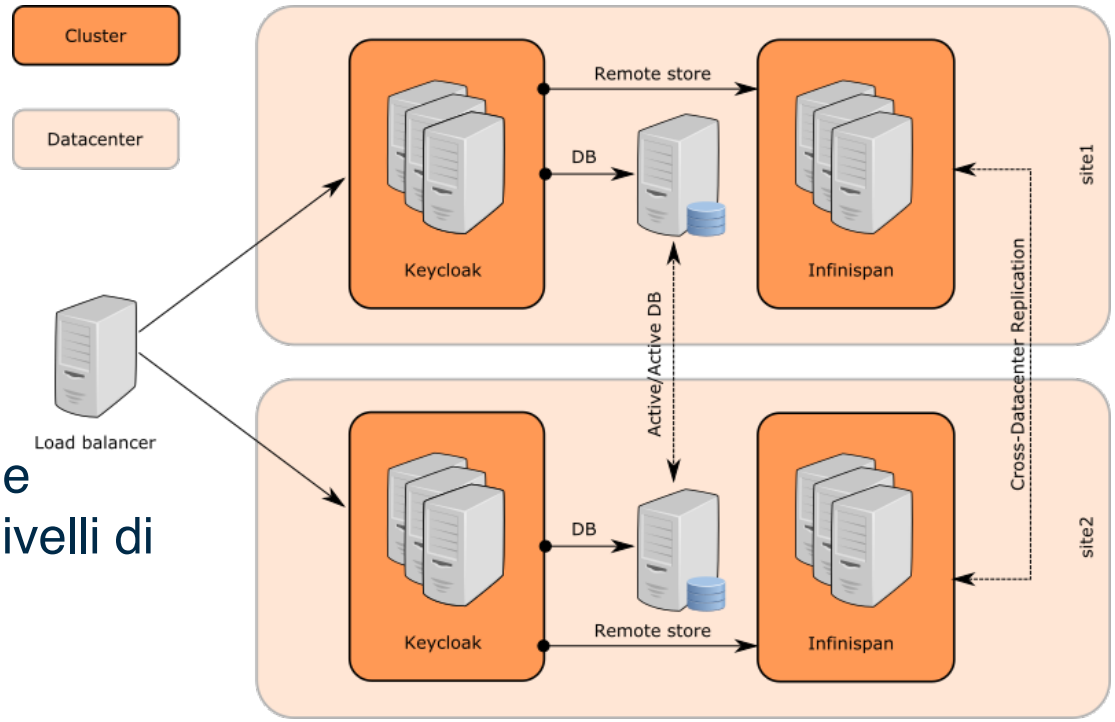


To cluster or not to cluster…

- AuthN & AuthZ SAML
  - Distribuita
  - Scalabile
  - Fault-tolerant
- OIDC non può avere caratteristiche differenti

To cluster or not to cluster…

- AuthN & AuthZ SAML
  - Distribuita
  - Scalabile
  - Fault-tolerant
- OIDC non può avere caratteristiche differenti
- Cluster Keycloak per HA e scaling può raggiungere livelli di complessità elevati



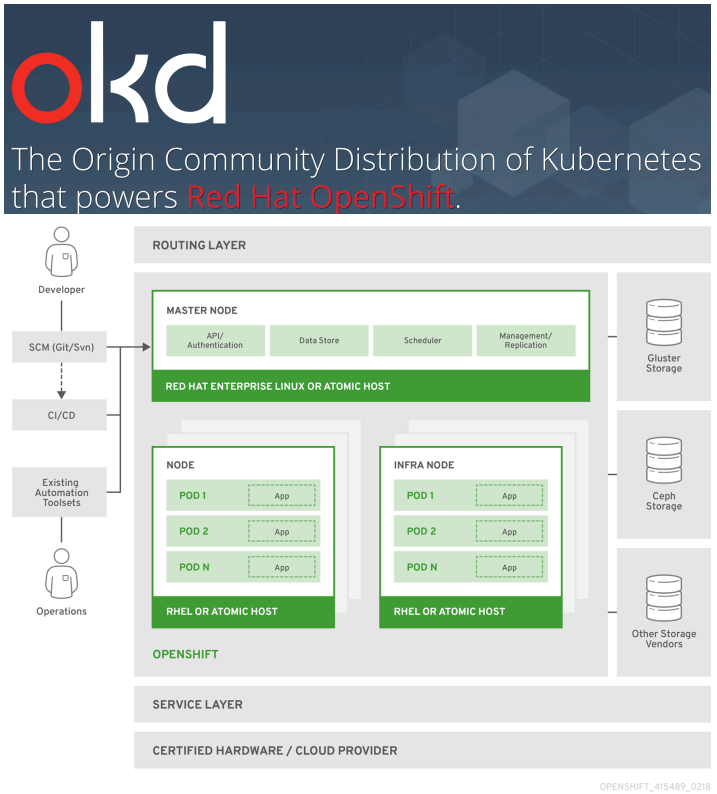
Il mio cluster è differente…

Il mio cluster è differente…

- Cluster OKD per supporto allo sviluppo ed erogazione di servizi web con architettura a microservizi.

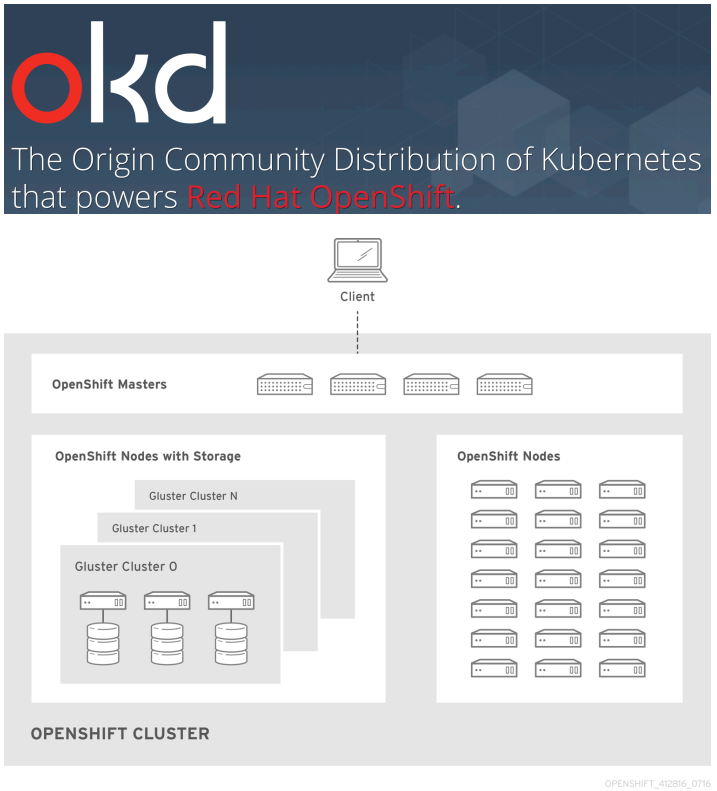
Il mio cluster è differente…

- Cluster OKD per supporto allo sviluppo ed erogazione di servizi web con architettura a microservizi.
- Architettura a layer per gestire e rendere fruibili immagini Docker



Il mio cluster è differente…

- Cluster OKD per supporto allo sviluppo ed erogazione di servizi web con architettura a microservizi.
- Architettura a layer per gestire e rendere fruibili immagini Docker
- Implementabile a partire da una manciata di nodi
  - 1 master
  - 3 infrastruttura
    - GlusterFS, router, worker
- Scale-up semplice ed indolore (a caldo)



Keycloak Docker Image in OKD

- Disponibile immagine docker

```
docker pull jboss/keycloak
```

Keycloak Docker Image in OKD

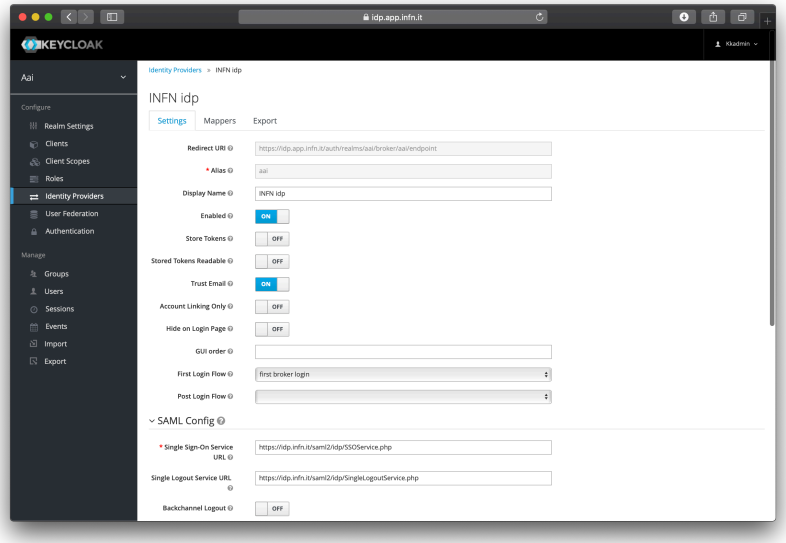
- Disponibile immagine docker
- Il servizio in OKD richiede la definizione di
  - DataBase, con relativo volume (su storage GlusterFS) e regole di accesso
  - Rotta di accesso al servizio Keycloak e regole di accesso alla console

```
docker pull jboss/keycloak
```

```
keycloak_deployment.yaml
keycloak_route.yaml
keycloak_secret.yaml
keycloak_service.yaml
postgresql_deployment.yaml
postgresql_secret.yaml
postgresql_services.yaml
postgresql_volume.yaml
```

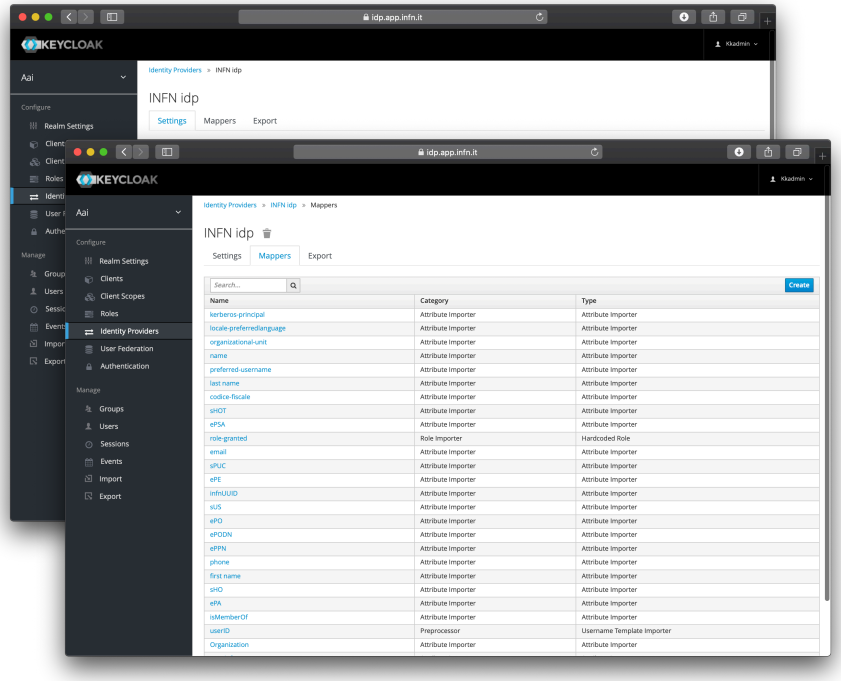
Keycloak SAML to OIDC Identity Broker

- Si configura Keycloak come SP SAML



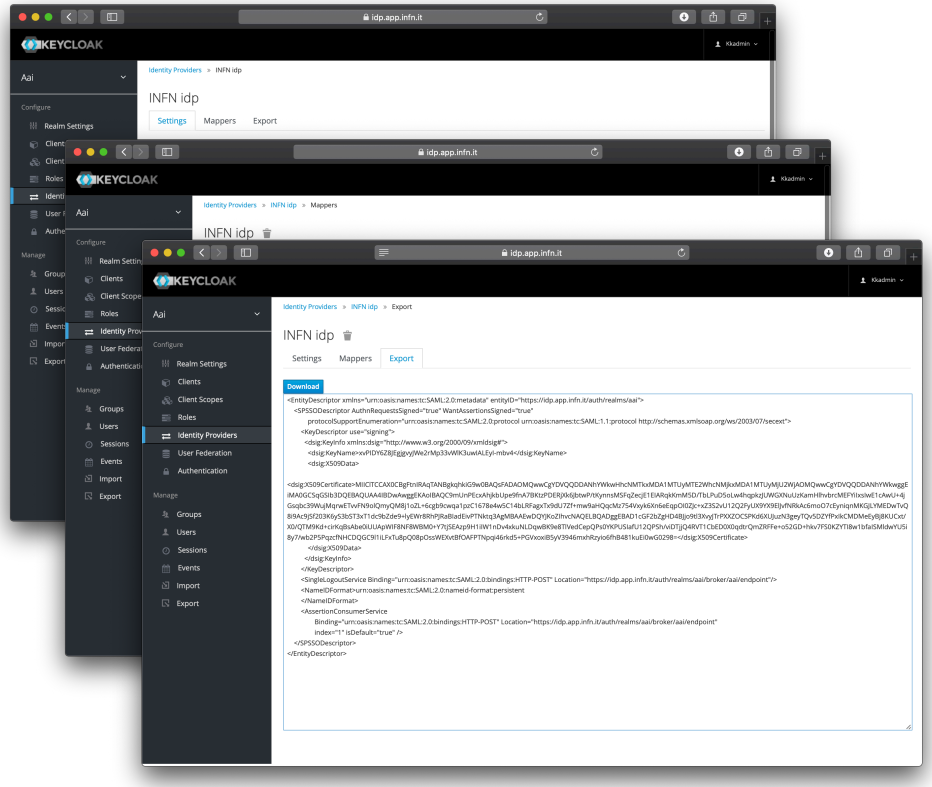
Keycloak SAML to OIDC Identity Broker

- Si configura Keycloak come SP SAML
- Si definiscono i «mapping» per gli attributi



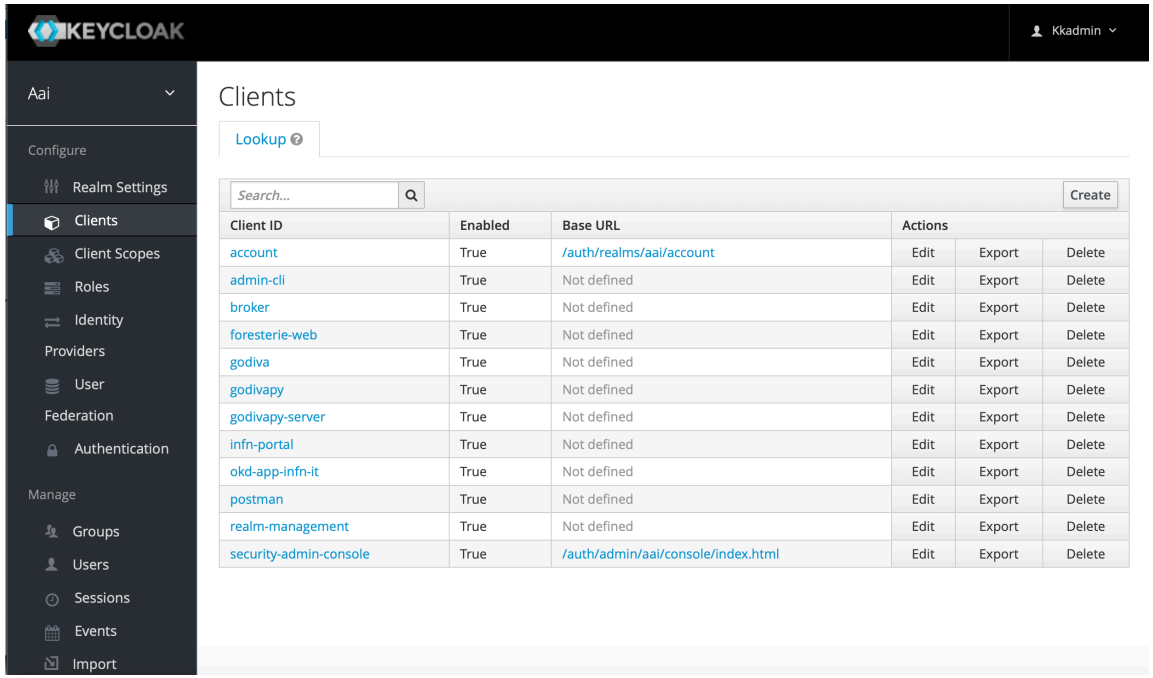
Keycloak SAML to OIDC Identity Broker

- Si configura Keycloak come SP SAML
- Si definiscono i «mapping» per gli attributi
- Si registra l'SP nell'IdP SAML



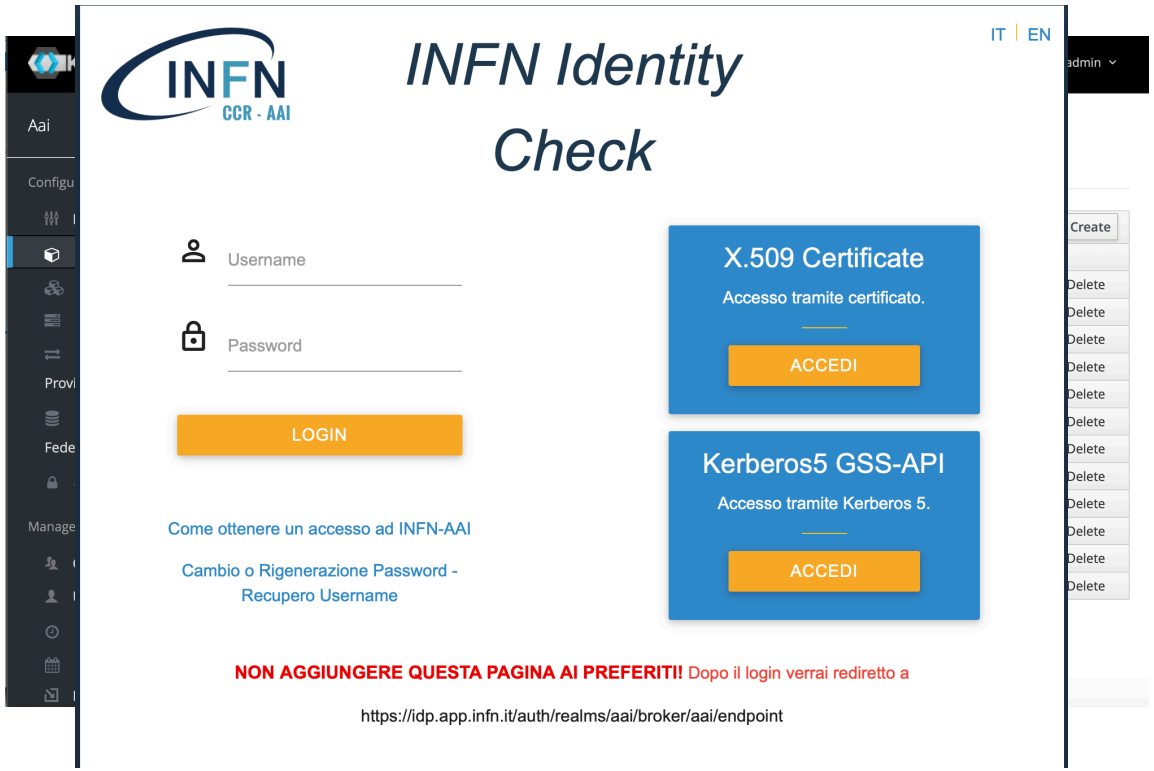
OIDC Client: browser flow

- account
  - OIDC client a corredo in Keycloak
  - /auth/realms/aai/account



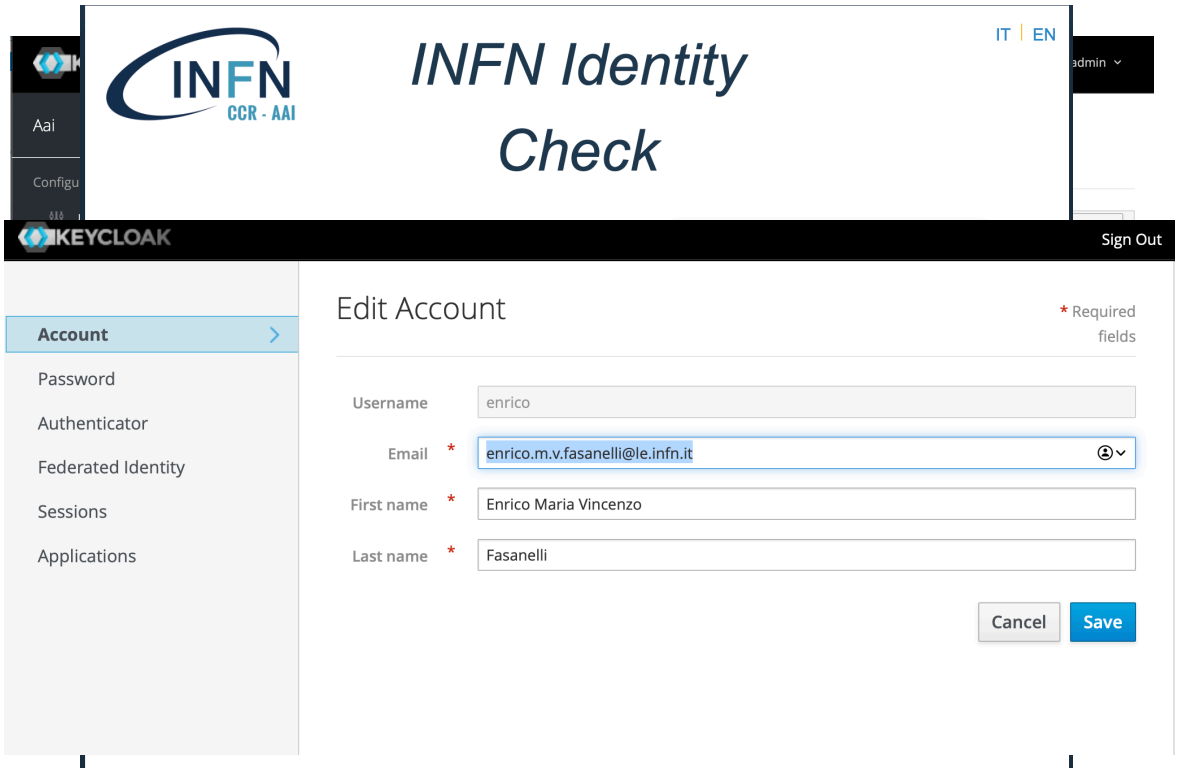
OIDC Client: browser flow

- account
  - OIDC client a corredo in Keycloak
  - /auth/realms/aai/account
- Redirect verso IdP SAML



OIDC Client: browser flow

- account
  - OIDC client a corredo in Keycloak
  - /auth/realms/aai/account
- Redirect verso IdP SAML
- First-login flow



Command Line Interface

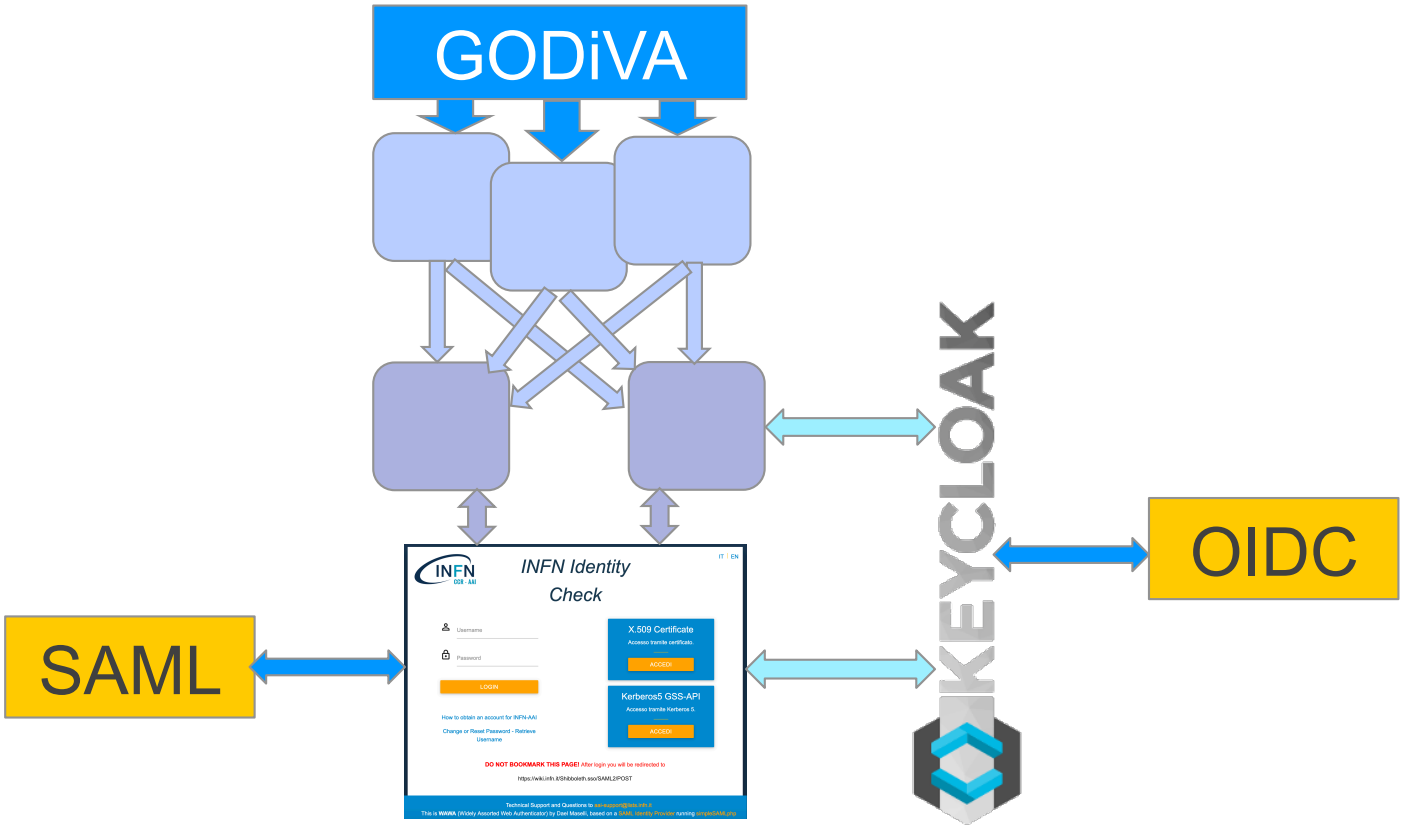
- CLI e script sembrano essere tagliati fuori da questo ambiente, ma i system admin INFN ne hanno bisogno

Command Line Interface

- CLI e script sembrano essere tagliati fuori da questo ambiente, ma i system admin INFN ne hanno bisogno

- OIDC Direct Grant Flow
  - LDAP back-end
- AuthZ
  - username/password
  - Kerberos

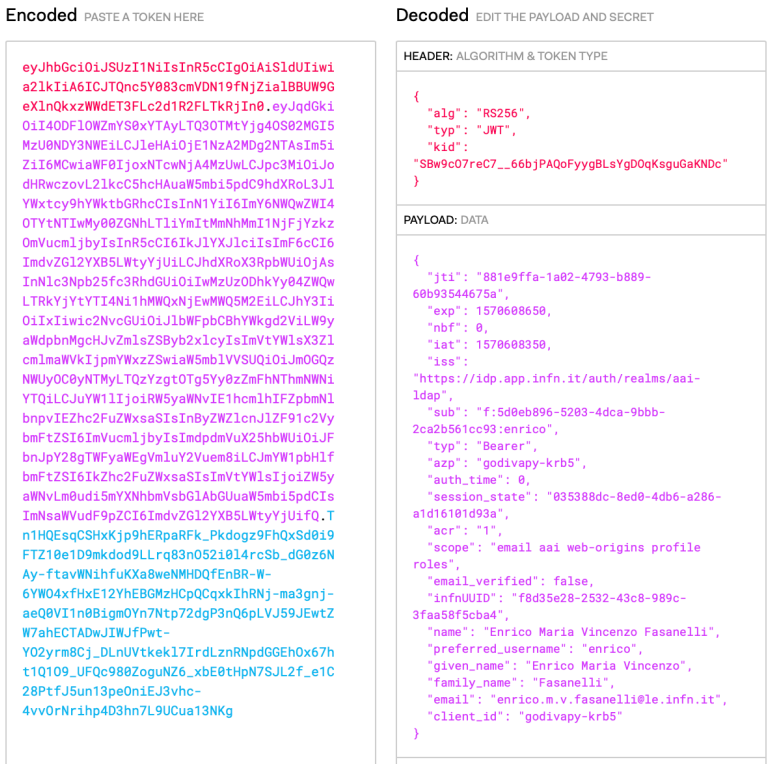
Architettura SAML + OIDC



Production-ready

curl -X POST -d 'grant_type=password' -d 'client_id=godivapy-krb5' --negotiate \
-u : https://idp.app.infn.it/auth/realms/aai-ldap/protocol/openid-connect/token

eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJTQnc5Y083cmVDN19fNjZialBBUW9GeXlnQkxzWWdET3FLc2d1R2FLTkRjIn0.eyJqdGkiOiJiZGUwYWNjNy01NDFmLTQ3M2ItOTcwNy03NGMwNjAwYmM0NjEiLCJleHAiOjE1NzA2MDkwOTMsIm5iZiI6MCwiaWF0IjoxNTcwNjA4NzkzLCJpc3MiOiJodHRwczovL2lkcC5hcHAuaW5mbi5pdC9hdXRoL3JlYWxtcy9hYWktbGRhcCIsInN1YiI6ImY6NWQwZWI4OTYtNTIwMy00ZGNhLTliYmItMmNhMmI1NjFjYzkzOmVucmljbyIsInR5cCI6IkJlYXJlciIsImF6cCI6ImdvZGl2YXB5LWtyYjUiLCJhdXRoX3RpbWUiOjAsInNlc3Npb25fc3RhdGUiOiIxMWU5MzFmZS1iMzg1LTQwMGYtOWRkNC0xOTYxNjNjY2U2YzUiLCJhY3IiOiIxIiwic2NvcGUiOiJlbWFpbCBhYWkgd2ViLW9yaWdpbnMgcHJvZmlsZSBvZmZsaW5lX2FjY2Vzc1wiLCJlbWFpbF92ZXJpZmllZCI6ZmFsc2UsImNsaWVudF9pZCI6ImdvZGl2YXB5LWtyYjUifQ.eZeR4WfVe-oksuZQuQhdK_cnNBd6E0yp7M-LLpHrAAOdNqka-N2Fj26BEfTg5MFHTIJtCkmDmfXixMQIhHxaHrMs6O_1h51sG3qk-wIy6HNJnP3iH8o5ZTF5bVYAyU05Fk6JH5ilzTh-PBtvXlJ2pvEooTDM7A92g2gJ5kDSwRyggu0Jewq3jtbMMhYe2jZdLhi1qtbrjGpEjpHQMwlSCqxYM08WsbbwGqjC1N1JhY4ttV3bJAzAvZTgFSAkRt5cTVSuRAuZeXzL9TQhjUZEXmlp3w2a4ZGc9d8fx6IosZGwBq5DogxON6985y1FCVawWr0SUMtYPiM1EWEBgNng2Q



Grazie

- Ai colleghi INFN
  - Gruppo di Lavoro e gestione di INFN-AAI
  - Gruppo di gestione dei SSNN INFN
  - Gruppo di gestione delle reti del CNAF
  - Gruppo di Lavoro e gestione dell'infrastruttura OKD
  - Gruppo di sviluppo dei microservizi
  - Gruppo INDIGO-DataCloud per il suggerimento su Keycloak

A tutti voi per l'attenzione